Information Security Policy Handbook

for

TopSource Infotech Solutions

(Department of Information Technology)

Registered Address - Gama 1 3rd floor, GigaSpace
Viman Nagar | Pune 411 014
Tel: 020 67637117

	Designation	Department	Date
Authored by	IT Support Manager	Information Technology	01/07/2010
Approved by	Operations Director	Information Technology	05/07/2010
Released by	Operations Director	Information Technology	05/07/2010

Document	Information Security Policy Handbook
Current Version	V2.9
Prepared by	IT Support Manager
Document creation date	July 01, 2010

Modification History

Sr. No	Description of change	Date of change	Version no
1	Policy created	09/11/2009	1.0
2	Password policy added.	09/11/2010	1.1
3	Document classification policy added	02/12/2009	1.2
4	Backup restore procedure added for servers	07/07/2010	1.3
5	DR section updated	07/07/2010	1.4
6	Backup procedure for SQL Server added	08/07/2010	1.5
7	3rd party contractors policy added	29/07/2010	1.6
8	ISP contact details & 3rd Party contractors/vendors policy added	02/08/2010	1.7
9	Server & Workstation PM checklist added	09/08/2010	1.8
10	Procedure added for issuing Access card to new joinee	23/08/2010	1.9
11	Social Networking Media acceptable usage policy added	06-08-2013	2.0
12	Internet connectivity switchover process added	12/11/2013	2.1
13	Data retention policy added	15/01/2014	2.2
14	Power supply and UPS	19/02/2014	2.3
15	Server Security Policy added	22/04/2014	2.4
16	Internet connectivity (Alternate) details updated	11/03/2015	2.5
17	Policy Reviewed	17/11/2015	2.6
18	Removable Media Policy added	03/03/2016	2.7
19	Policy Reviewed	19/06/2017	2.7

20	Policy Reviewed	07/05/2018	2.7
21	Policy Reviewed	15/05/2019	2.7
22	Antivirus policy updated	28/01/2021	2.8
23	Remote work policy	29/01/2021	2.9
24	Contact information updated	21/12/2021	3.0

CONTENTS

1. Introduction

This Information Security Policy document outlines the business rules for protecting information and the systems which process the information. This document provides a high level description of various controls that TopSource has in place to protect both internal and client data.

For the purpose of this document, Information Security is defined as protecting information and information systems from unauthorized access, use, disclosure, loss, removal, disruption, modification or destruction. The goal of information security is to protect the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, etc.

This document is comprised of procedures, standards and guidelines that are incorporated into and are part of TopSource Global Solution's Information Security Policy.

2. Background

TopSource is a leading provider of accounting and payroll solutions to India and UK companies. We are a privately-held group and operate from three main delivery offices. We ensure that each TopSource client receives the right service in the right way. Our 533 active clients range in size and cut across every major industry.

Each client has a dedicated account owner and a company director who is personally responsible for the services delivered.

We have no sales people between our commitments and our services, ensuring that any commitment that is made is adhered to by the people making it.

At TopSource, we have clearly defined strategic objectives that support every aspect of our business. Each strategy is underpinned by our Corporate Strategy and must adhere to our Company Values. Every TopSource colleague learns and lives our values.

Our values

Promised Service: We will be clear about what we will do for our clients, and what we expect of them. Delivering the promised service will require us to do what we say we are going to do, when we said it would get done, and we will do it according to our documented processes to achieve the expected outcome. This will include internal clients and external clients.

Pricing integrity: We will charge only what we quote. We will use clear and precise pricing language (and put this in writing) for our clients to confirm what we will charge, when we will charge, and when we expect to get paid.

Accountability: We are accountable for our work, our actions and our omissions. When we err, we take responsibility and raise any errors to the party impacted by the error. When we excel, we celebrate the success of our colleagues and our company.

Credibility: We have the skills and infrastructure to achieve our objectives and to deliver the promised service. We will ensure that our colleagues have the skills to do their job right.

Respect: We will treat our colleagues, clients and partners with respect by being direct and open about issues, opportunities and our understanding of responsibilities. We will expect the same in return.

Flexibility: When our clients come to us with a payroll or accounting challenge, we will always seek to create and deliver the solution.

TopSource facts

TopSource has 194 colleagues operating across our three offices.

We deliver services to 533 clients across four brands that each services specific markets.

TopSource UK is the parent company of the Group. TopSource services mid-market UK companies. Services include accounting support services and payroll outsourcing services. Flexibility, accountability and personalised client support are the hallmarks of the TopSource *promised service*. To learn more, visit us at https://topsourceworldwide.com/

Practical Payroll Solutions (PPS) is a TopSource subsidiary. The business has deep expertise in large and complex payrolls. PPS supports clients throughout the entire payroll process lifecycle.

PPS has particular expertise in government and facilities management. To learn more, visit us at www.ppay.co.uk

TopSource India provides services to India-based clients. With over 85 clients, the operations support payroll outsourcing services to over 30,000 employees every month. India-based clients are served with leading-edge technology that allows for individualised support and employee-level engagement. To learn more, visit us at https://topsourceworldwide.com/services/india-payroll/

Portico is our proprietary HR and document workflow system. Portico is available to every TopSource client and is accessible as a centralised or employee-self-service application. To learn more, visit us at https://portico.topsource.in OR www.myportico.co.uk

TopSource Global Solutions provides payroll, accounting and administrative services to its customers. As part of the provision of these services employee pay information, accounting information and personal data of its clients are stored and processed by TopSource. The data is received by TopSource in a variety of formats including paper, email, scanned PDF files, and fax. In many cases, TopSource accesses client information via bespoke application systems over the Internet.

This document outlines the controls that have been implemented to protect the customer data that is both received and accessed by TopSource.

The objective of this Information Security Policy Handbook is to provide a comprehensive framework for:

- Protecting the confidentiality, integrity and availability of TopSource information assets and information resources.
- Ensuring the effectiveness of Information Security controls over information assets and information resources that support TopSource's operation.
- Recognizing the highly networked nature of the current computing environment and to provide effective company-wide management and oversight of information related security risks.
- Provide for development and maintenance of minimum controls required to protect information assets and resources belonging to TopSource and its clients.

- Provide a mechanism for continuous evaluation of security and controls.

3. Scope

The Information Security Policy Handbook is comprised of policies, procedures, standards and guidelines that apply to all employees, contractors, sub-contractors, consultants, temporary workers, guests and any third-party individual/company that utilize TopSource information assets or information resources. All information assets and information resources used by and in support of TopSource business operations must comply with the provisions of this policy.

The scope of this document is to address the approach to Information Security via the following key principles.

4. Confidentiality

For the purpose of this document, confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. Unauthorized individuals may be TopSource employees or others. This policy outlines the controls in place to prevent unauthorized access or unintentional modification to Information Systems and the data stored thereon.

The policy is applicable to all TopSource computing resources such as desktops, laptops, servers, communication equipment's where TopSource staff manages access control. The term "user" in policy includes employees, contractors, trainees, vendors, partners and suppliers who are may access TopSource's computing resources.

4.1 User Access Control

- TopSource offices have 24 hour manned security with an employee/visitor sign-in/sign-out register. Access control cards are issued to all authorized users.

- User access to application resources are granted based on business requirements; on a "need to access" and "need-to-know" basis. IT Manager and Software Manager provide access to IT resources and access to applications based on instructions from Project Managers.

- Third party access to contractors, customers, trainees is permitted after due authorization from Program Managers. All visitors are escorted in to the office by employee or authorized person to work area.
- The Admin Manager issues access cards on authorization from the HR manager for new employees. The Admin Manager maintains a register of all electronic access cards and the persons to whom they are issued. When employees leave, the HR manager ensures that the card is returned by the employee.
- Access to visitors or any persons without an access card need to sign in the visitors register and need to be escorted to a meeting/work area in the secure facility along with an employee.
- Access to the Server Room is restricted to the IT team via electronic access card system that allows access to only IT team members. Access to employees/third party contractors to the Server Room is allowed after entry into a Server Room Visitor register and the employee is escorted in and out by an IT team member.
- Users are required to read and sign applicable customer specific Non-Disclosure Agreements (NDAs) along with any other associated agreements before being provided with any physical or logical access to a particular project/resource.
- Users are required to be aware of their access rights and associated responsibilities.
- User access is limited by time period as required.
- Users are made aware of the need to protect critical information (Documents/Media) under possession, from unauthorized physical and logical access.
- The Desktop Security Policy is outlined in Appendix 3.

4.2 Sensitive Equipment and Server Setting Protection

- All sensitive equipment and servers are deployed in dedicated server rooms, which are secured with biometric locks. Servers and other equipment are password protected. Physical and logical access codes are in the possession of the dedicated IT team and are regularly changed by the IT administrator.
- USB ports, CD/DVD and disk drives are disabled from all the user workstations.
- All paper printouts are securely shredded. See Appendix 2 for the data destruction policy.

5. Integrity

For the purpose of this document, integrity is the term used to ensure that data cannot be modified without authorization.

5.1 Password Policy

Important Note: *The following policy is considered as the minimum baseline password policy for implementation across all IT systems in TopSource. More stringent criteria for setting and usage of passwords can be implemented for identified IT Infrastructure based on the need.*

TopSource follows the best practices on passwords usage and strictly adhere to the password policy as described below:

- Passwords will be changed every 45 days
- Passwords will be a minimum of 8 characters.
- Passwords will be alphanumeric characters with a minimum of 2 numeric characters.
- Blank passwords are not permitted.
- The minimum password age will be 1 day. There may be no immediate changes of passwords.
- Guest accounts will be removed on installation of systems.
- Default system accounts provided by vendor/service provider must be renamed upon installation of new systems.
- Last 5 passwords may not be reused for any reason. After 5 unsuccessful attempts, an account is locked until the system administrator reactivates the account.
- Responsibility of maintaining confidentiality of user passwords is communicated as critical to the user.

5.2 Network Access Control

- Every client node (external visitor, new hardware purchased and current nodes) is checked for viruses or malware and updated with latest software patches before connection to the TopSource network.
- If any kind of ambiguity is found, the client node is transferred to an isolated network, made compliant as per the security policy and then given access to the network.

- Users are not allowed to connect any new resources onto the network without prior approval from a Project Manager and the IT Support Team.
- Network connectivity from user desktop to local servers and to the remote networks/systems is controlled/restricted/monitored by the System Administrator/ IT Support Team.
- The TopSource network has the appropriate secured gateways/firewall to segregate internal and external domains and also to isolate customer networks.
- Implementation of gateway level anti-virus filtering for protection against viruses is in place.

5.3 Operating System Access Control and Application Control

- Operating systems and applications are configured to run only restricted services as required.
- Operating systems and applications are fine-tuned to run only the required services and access for intended project use.
- Systems keep a log of unsuccessful attempts and the designated System Administrator reviews the log as needed.
- All desktop resources are identified by the unique identifier (e.g. UID, User ID).

5.4 Anti-virus System and Security Patch Update

All workstations and servers are loaded with anti-virus software which is updated daily and managed and controlled centrally by the System Administrator. All machines are thoroughly scanned weekly.

WSUS server is in place, which delivers regular security/critical updates to all workstations and servers. See Appendix 1 for more details.

5.5 Firewall

Hardware and software firewalls are installed in the TopSource network which prevents any unauthorized access from outside of TopSource domain. The firewalls contain IPS/IDS (Intrusion Detection System/Intrusion Prevention System), gateway level anti-virus, anti-spyware, and application firewalls.

Access to unauthorized websites is prevented using a URL filter. Downloading of unauthorized attachments and software (.exe, .zip, .rar, etc.) is prevented using these firewalls.

Regular maintenance and firmware updates are carried out by the System Administrators.

5.6 Internal/External Security Audit

Internal security audits of systems, servers and firewalls are carried out by the IT Team every three months.

External security audits of systems, servers and penetration testing of firewalls are carried out by an external qualified audit agency once a year.

5.7 Data Classification

A Data Classification Policy exists to classify data according to the risks associated with its storage, processing, and transmission. Consistent use of this data classification policy facilitates efficient business data processing and lowers the costs of ensuring adequate information security. See Appendix 4 for more details.

5.8 Email Usage Policy

Appendix 5 outlines suggested company rules and procedures and employee responsibilities for electronic mail (e-mail) messages sent or received via the TopSource e-mail systems.

5.9 Mobile Computer Policy

Appendix 6 defines a policy for use of mobile computers in the organization.

5.10 Managing 3rd party contractors

Appendix 8 outlines the approach for managing 3rd party contractors / vendors.

6. Availability

For any information system to serve its purpose, the information must be available to authorized individuals when required. The computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

The dedicated IT support team monitors availability. These activities are outlined below.

6.1 Current Practices & Procedures

An understanding of the operational practices currently followed by the IT department is essential to recovering systems and applications. The key activities include:

- Data backup & restoration
- Server & systems administration
- System shutdown and startup
- Identification of critical systems
-

6.2 Data Backup & Restoration

The incremental backup all servers are performed daily and this incremental backup is restored on an off-site backup server every day.

A restore drill procedure is followed once every 3 months with the off-site backup server restore and test the backup.

6.3 Server & System Administration

Current practice for managing servers and desktop systems across the company includes:

• Ensuring high availability of servers during business hours.
• User support and desktop system support from06:30 AM to 10:30 PM IST.
• Other major server maintenance is scheduled outside of normal business hours.

6.4 Server & Workstation preventive maintenance process

Appendix 9 outlines process to carry out Server maintenance and workstation procedure.

6.5 Recovery Operations

The recovery process consists of two basic phases:

1. Data Recovery – Data recovery involves restoring of data from offsite backup server.
2. System Recovery – System recovery involves restoring the operating system.

6.6 System Shutdown & Startup Procedures

System shutdown and startup procedures for all critical systems including all servers and telecommunications systems have been developed.

Systems run on a 24x7 basis and shut down only for the following reasons:

1. Critical patch upload (i.e. virus definition update sometimes requires reboot). Typically, systems are rebooted only on weekends by rescheduling backups.
2. Hardware or OS/Application upgrade.
3. Maintenance of hardware.

6.7 Internet Connectivity

Internet connectivity in TopSource is highly available through redundant connections. TopSource uses an 8Mbps dedicated leased line connection from the predominant vendor as primary internet line. The connectivity utilizes a fiber link which is a redundant using loop back connectivity.

Redundant internet of 8Mbps connectivity is provided from another internet service provider (ISP).

Both the lines are terminated in two separate routers and procedure exists to automatically switchover internet connectivity in the event of primary line goes down. This is an automated process and is transparent to end user.

6.8 Authenticity and Non-repudiation

For the purpose of this document, authenticity is the term used to ensure that data, transactions, communications or documents (electronic or physical) and the parties accessing the data are genuine.

TopSource provides data access to clients through a bespoke and proprietary document archival system – Portico. All access to Portico is password protected and the transmission of data to and from the archive is encrypted.

6.9 Power Supply and UPS backup

Two separate UPS systems provide un-interrupted power supply to all the workstations in both A and B wing separately. These two UPS systems are configured with two 15KVA UPS and in the event of failure of one UPS other UPS can take part of load.

Two separate UPS systems are installed in server room. One UPS provides supply to all critical servers and network devices. Second UPS provide power supply for other remaining miscellaneous devices and non-critical servers and workstations. These UPS system can provide up to 8 hrs. Power supply in the event of main power supply fails.

All the UPS are backed up with DG backup provided by Giga Space and are automatically switchover when power supply from MSEB fails.

7. Risk Management

Risk Management identifies the vulnerabilities and threats to information resources used by TopSource and outline the countermeasures, if any, to ensure business continuity.

Risk management is not part of the scope of this document. It is addressed as part of the Business Continuity Plan of TopSource.

8. Policy and Documentation Review

TopSource will review the adopted Information Security Policy annually at a minimum. The purpose of the review is to ensure the continued suitability, adequacy and effectiveness of the policies. TopSource will review the Information Security Policy on a more frequent basis particularly if significant changes occur within their organization that may have an impact on the effectiveness of the policy.

9. Appendix 1 - Antivirus Computer Policy

9.1. Introduction

This policy is an internal IT policy of TOPSOURCE which defines anti-virus policy on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what anti-virus program will be run on servers and workstations. It also specifies how files can enter the trusted network and how these files will be checked for hostile or unwanted content.

9.2. Purpose

This policy is designed to protect the organizational resources against intrusion by viruses and other malware.

9.3. Anti-Virus Policy

The organization will use a single anti-virus product for virus protection and that product is **Trend Micro Office Scan Antivirus**. The following minimum requirements shall remain in force.

- The anti-virus product is operated in real time on all servers and client computers. The product is configured for real time protection.
- The anti-virus library definitions are updated at least once per day.
- Anti-virus scans are done a minimum of once per week on all user-controlled workstations and servers.
- The computer nodes which are not connected/reported to server for 30 days are automatically removed from the managed client list from server console. These node will still receive the update from internet and will be added to server managed client list when connected to server successfully.

No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

9.4. Email Server Policy

When a virus is found or malware is found, the policy is to delete the email and not to notify either the sender or recipient. The reason for this is that most viruses fake the sender of the email and sending them a notice that they sent a message with a virus may alarm them unnecessarily since it would not likely be true. It would simply cause an additional help desk call

by the notified person and most likely waste system administrator's time needlessly. Notifying the recipient that someone tried to send them a virus would only alarm them needlessly and result in an increased number of help desk calls. The antivirus software used does this automatically.

9.5. File Exchange Policy

This part of the policy specifies methods that are allowed to be used when files are sent into the network by members of the public or employees of the organization.

The following methods are allowed:

- FTP transfer to a FTP server after user authentication.
- File transfer to and from Web Server uses 128-bit Secure Socket Layer (SSL) technology to encrypt information. The information is encrypted on computer, sent through the Internet as jumbled code, and decoded on our server. It cannot be read in transit.

10. Appendix 2 – Data Destruction Policy

10.1. Introduction

All the staff working with TOPSOURCE has personal responsibility to keep client and other information secure and confidential. There are several important issues to bear in mind when transferring information, particularly in electronic format (emails, CD, DVD etc).

This Policy aims to prevent unauthorized disclosure of information assets by the controlled disposal and destruction of sensitive data.

10.2. Purpose

This procedure covers how TOPSOURCE ensures the destruction of all customers' data and to show how this is maintained and logged at all stages.

Following are the most common forms of media currently in use which can contains information and need to be destroyed.

Media Types

- Hard Disk Drives
- CDROM/DVR-R
- CD-RW/DVD-RW
- Magnetic Tape
- Flash Disk Drives
- Paper

10.3. Removal of Data

Data Removal from Live Systems

There are various scenarios in which data may need removing from a system while still in operation, or reuse of the media is required for financial or policy reasons.

In these cases, we make all possible efforts to remove the required data from the target media. In this case, the most common scenario would be to remove the data from hard disks, or tape backup devices, when a particular application no longer requires it.

Data Removal for Media Reuse

Often, media such as hard disk drives are reused rather than completely decommissioned. In the case of reuse, system administrators will clear all the data on hard disk, and ensures the data is non-recoverable .The reuse of disk is then done within the office premises and the disk does not go outside office premises.

10.4. Media Destruction Techniques

Media, which is no longer required (or has passed its effective reuse period), is destroyed.

Hard Disk Destruction

Complete physical destruction of the hard disk device is required to ensure that any recovery of data is impossible.

Hard disk devices are physically destroyed using brute force methods. Putting appropriate safety methods in place, non-specialist staff destroys these devices. The outer casing requires removal and the internal circuitry is broken into tiny fragments (including any integrated circuit chips).

CD-ROM and DVD Destruction

The construction of plastic media such as CDs makes them particularly vulnerable to damage if handled roughly. Most CDs and DVDs are simply a plastic base with a laser sensitive substrate applied to one side.

Breaking the plastic base into small fragments, and disposing of the remains as normal waste, is done for non-sensitive data. We also use paper shredding machines for the destruction of CDs in this manner.

Solid-State Devices

Solid-state devices normally consist of Flash USB drives or memory storage cards for PDAs and other handheld devices. Due to the compact nature of their internal makeup, the complete physical destruction of the device is required to ensure that any recovery of data is impossible.

Devices such as USB thumb drives are physically destroyed using brute force methods. Putting appropriate safety methods in place, non-specialist staff destroys these devices. The outer casing requires removal and the internal circuitry is broken into tiny fragments (including any integrated circuit chips).

Magnetic Tape Backup

The most effective method for the destruction of magnetic tape is the disintegration or shredding of the tape media. Physical destruction of the tape is done subsequently.

Paper Based

We shred paper records through cross cut shredder that cuts the paper into pieces of no more than 15mm x 4mm.

11. Appendix 3 – Desktop Security Policy

11.1 Introduction

This Desktop security policy document outlines the measures employed to protect the desktop PCs and Laptops in the organization. This document provides Desktop security guidelines for the following:

- Hardware Security.
- Access Level Security.
- Data & Software availability.
- Confidential Information.

11.2 Purpose

This policy is created for the purpose of defining guidelines for physical security as well as data security on the desktop and Laptop PCs of the organization.

11.3 Scope

This policy applies to all who uses desktops and laptops in TopSource.

11.4 Access Level security

- Passwords are used to ensure that only authorized users can gain access to the system.
- Screen gets locked after the keyboard and/or mouse have been idle for a period of 10 minutes.
- User accounts set on desktops and laptops are not assigned to the 'Administrators' group. All users are designated as a 'Restricted' or 'Power' user.

11.5 Data and Software Availability

- Users are expected to use the desktop storage media only for temporary storage. All Final reports and outputs are stored on the file servers in the designated area for the specific client.
- Only standard approved software is installed on the system. All software installations are performed by system administrators.
- Approved anti-virus software is installed and maintained on each desktop and laptop computer. IT support staff is responsible for applying the most current definitions which are updated on a regular basis. Scheduled scanning for viruses is performed weekly.

- No passwords are stored in clear text and visible to others on any desktop system, nor are they shared among staff members.
- VPN software is installed on client workstations for users requiring remote access via the Internet.

12. Appendix 4 Document Classification Policy

12.1 Introduction

This Document classification policy outlines the classification of documents in the organization and the steps taken to protect critical data in the organization.

12.2 Purpose

The purpose of the Data Classification Policy is to provide a system for protecting information that is critical to the organization, and its customers. In order to provide more appropriate levels of protection to the information assets entrusted to TOPSOURCE, data is classified according to the risks associated with its storage, processing, and transmission. Consistent use of this data classification policy facilitates efficient business data processing and lowers the costs of ensuring adequate information security.

12.3 Scope

The Data Classification Policy applies equally to any individual, or process that interacts with the organization's information resources in any tangible manner. All personnel who may come in contact with confidential information are expected to familiarize themselves with this Data Classification Policy and consistently use it.

12.4 Policy

Responsibility for Data Management

Data is a critical asset of TOPSOURCE, its business partners, and its customers. All individuals employed by TOPSOURCE have the responsibility to protect the Confidentiality, Integrity, and Availability of the data generated, accessed, modified, transmitted, stored and/or used by TOPSOURCE, irrespective of the medium on which the data resides and regardless of format (i.e. electronic, paper or other physical form).

Data User

The Data User is a person, organization or entity that interacts with data for the purpose of performing an authorized task. A Data User is responsible for using data in a manner that is consistent with the purpose intended and in compliance with the policy.

Data Owner

The Data Owner is normally the person responsible for, or dependent upon the business process

associated with an information asset. The Data Owner is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.

- The Data Owner determines the appropriate value and classification of information generated by the owner or department;
- The Data Owner communicates the information classification when the information is released outside of the department and/or TOPSOURCE.
- The Data Owner controls access to his/her information and is consulted when access is extended or modified.
- The Data Owner communicates the information classification to the Data Custodian so that the Data Custodian can provide the appropriate levels of protection.

Data Custodian

The Data Custodian maintains the protection of data according to the information classification associated to it by the Data Owner.

Data Classification

Data owned, used, created or maintained by TOPSOURCE is classified into one of the following three categories:

- Public
- Internal
- Confidential

Public Data

Public data is information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to TOPSOURCE disclosure rules, is available to all TOPSOURCE employees and all individuals or entities external to the corporation.

Examples of Public Data include:

- Publicly posted press releases
- Publicly available marketing materials
- Publicly posted job announcements

Disclosure of public data is made ensuring that it does not violate any pre-existing, signed non-disclosure agreements.

Internal Data

Internal Data is information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute

requiring this protection. Internal Data is information that is restricted to personnel designated by TOPSOURCE who have a legitimate business purpose for accessing such data.

Examples of Internal Data include:

- Employment data
- Business partner information where no more restrictive confidentiality agreement exists
- Internal directories and organization charts
- Planning documents
- Contracts

Internal Data:

- Is protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
- Is protected by a confidentiality agreement before access is allowed.
- Is stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
- Is destroyed when no longer needed subject to the TOPSOURCE Data Retention requirement. Destruction may be accomplished by:
  - "Hard Copy" materials are destroyed by shredding which destroys the data beyond recognition or reconstruction as per the TOPSOURCE Data Destruction and Re- Use Standard.
  - Electronic storage media are sanitized appropriately by overwriting prior to disposal.

Confidential Data

Confidential Data is information protected by statutes, regulations, TOPSOURCE policies or contractual language. Managers may also designate data as confidential. Confidential Data is sensitive in nature, and access is restricted. Disclosure is limited to individuals on a "need-to-know" basis only.

Examples of Confidential Data include:

- Safety data
- Social Security Numbers / NI numbers / PAN numbers
- Personnel and/or payroll records
- Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction
- Any data belonging to a TOPSOURCE customer that may contain

- Personally identifiable information
- Patent information
- Regulatory filings

Confidential Data:

- When stored in an electronic format is protected with a minimum level of authentication to include strong passwords, wherever possible.
- When stored on mobile devices and media has protection and encryption measures provided by IT Management.
- When sent via fax, is sent only to a previously established and used address or one that has been verified as using a secured location.
- Is not posted on any public website.
- Is destroyed when no longer needed.

Data retention

TopSource retains data marked as internal and confidential for eight years.

After data retention period is over, data is securely destroyed.

13. Appendix 5 – Electronic Mail Policy

13.1 Introduction

This document outlines suggested company rules and procedures and employee responsibilities for electronic mail (e-mail) messages sent or received via the TopSource e-mail systems.

13.2 Purpose

The purpose of e-mail is to conduct TopSource business.

13.3 Ownership

- E-mail equipment and messages are TopSource property.
- Messages that are created, sent or received using the company's e-mail system are the property of the TopSource.
- TopSource reserves the right to access and disclose the contents of all messages created, sent or received using its e-mail system.

13.4 Usage

- All e-mail communication must be handled in the same manner as a letter, fax, memo or other business communications.
- No copyrighted or company proprietary information is to be distributed by company e-mail unless approval has been granted by a company official.
- No commercial messages, employee solicitations, messages of a religious or political nature are to be distributed using company e-mail.
- E-mail messages may not contain content that may be considered offensive or disruptive. Offensive content includes but is not limited to obscene or harassing language or images, racial, ethnic, and sexual or gender specific comments or images or other comments or images that would offend someone on the basis of their religious or political beliefs, sexual orientation, national origin or age.
- Employees may not retrieve or read e-mail that was not sent to them unless authorized by the company or by the e-mail recipient.

13.5 Viruses and phishing

Emails can pose a security risk to business. They are often used to distribute viruses and spyware, or for phishing attempts.

Phishing is a type of fraud in which a hacker attempts to gather personal information or credentials by impersonating a legitimate brand and sending users to a malicious website.

An example would be an email with a generic greeting warning of a change in an account requiring you to verify your account information. These emails typically include directions to reply with private information or provide a link to a web site to verify your account by providing personal information such as name, address, bank account numbers, Social Security numbers, or other sensitive personal information.

Indicators of a phishing email:

- Name and email address don't match
- Attempt to prove legitimacy using words such as 'Official'
- Uses a real organization or company name but incorrect email address
- Poor grammar
- Unsolicited requests for personal information are a clear danger signal
- Misspellings

Follow below steps to avoid phishing attack –

- Never send passwords, bank account numbers, or other private information in an email.
- Avoid clicking links in emails, especially any that are requesting private information.
- Be wary of any unexpected email attachments or links, even from people you know.
- Look for 'https://' and a lock icon in the address bar before entering any private information.
- Have an updated anti-virus program that can scan email.
- Do not open attachment from unknown source. Always inform the IT team if you receive a suspicious attachment or if you suspect a virus has entered the system.

13.6 Non-Business E-mail

No personal business is to be conducted using TopSource e-mail.

13.7 Violations

- Violation of this policy will result in disciplinary action up to and including termination and/or legal action if warranted.
- Employees should report any misuse of the company e-mail system or violations of this policy to the appropriate company official.
- Other e-mail issues addressed in this policy or included as part of the company's overall information systems standards and procedures are:
    - Virus checking of attachments – Anti-virus scanner automatically scans all the incoming mails and deletes the mail if a virus is found. Employees are advised not to open any suspicious attachment/content of a mail and inform the IT team immediately.
    - Password protection – The personal mail boxes of users may be password protected.
    - Archival/storage of old messages – Old mails and mailboxes can be archived on request.
    - Use of distribution lists – E-mail distribution lists are designed to provide an easy way to create and maintain large E-mail mailing lists. These lists can be used for the one-way distribution of information, for E-mail based discussion, questions and answers, etc. Lists are created and “owned” by an E-mail user who manages the list’s behavior. It is the owner’s responsibility to manage the list’s subscribers.
    - Restricting use of "copy all" for sending or responding to messages – “Copy all” for responding or sending mails should be avoided. If a message has been sent to a list and one reader replies to the person who sent the message by using the reply feature that reply may be sent to everyone on the list. For example, a conference coordinator sends a reminder message to a list of 10 people who will be attending a conference. One of the respondents has a question about whether his or her registration has arrived and replies to the message using the reply feature. Since the original message was sent to a list, it is quite possible that using the reply feature will result in that individual's message being transmitted to all 10 people on the list instead of only to the original sender.

14. Appendix 6 – Mobile Computer Policy

14.1 Introduction

This policy defines the use of mobile computers in the organization. It defines:

- The process that mobile computers must go thru to leave the corporate network. Both the device and any sensitive data should be password protected.
- How mobile computers and devices will be protected while outside the organizational network
- The process that mobile computers must meet to enter the corporate network when being brought into a building owned by the organization.

14.2 Purpose

This policy is designed both to protect the confidentiality of any data that may be stored on the mobile computer and to protect the organizational network from being infected by any hostile software when the mobile computer returns. This policy also considers wireless access.

14.3 Scope

This policy covers any computing devices brought into the organization or connected to the organizational network using any connection method. This includes but is not limited to desktop computers, laptops, palm pilots, Notebook, Smartbook, Notebook PC, Ultra-Mobile PC, Tablet PC, Pocket Computer, Personal Digital Assistance (PDA), Mobile Phones/Blackberry and Handheld PC.

14.4 Special Note

To write this policy, data and the sensitivity of the data stored and viewed on the mobile computer is considered including:

- Email
- Data the user is working on that is stored locally.
- Data from the internal network that the user may access while the computer is outside the network.
- Considered loss due to:

  A. Theft

  B. Hard drive failure

14.5 Responsibility

The user of the mobile computer will accept responsibility for taking reasonable safety precautions with the mobile computer and agrees to adhere to this policy. The computer user will not be allowed to have administrative rights unless granted special exception by the network administrator. The user of the computer agrees not to use the mobile computer for personal business and agrees to abide by the organizational computer usage policy.

14.6 Reporting Loss or Damage

Employees at remote working locations must promptly report to their manager any damage to or loss of the computer hardware, software, or sensitive information which has been entrusted to their care.

14.7 Travel Considerations

Removal of Information**:**

Sensitive (confidential or secret) information can be carried on a mobile device after obtained approval of a Program Manager.

Public Exposure**:**

Sensitive (confidential or secret) information must not be read, discussed, or otherwise exposed in restaurants, on airplanes or trains, or in other public places.

Checked Luggage**:**

Employees in the possession of portable, laptop, notebook, palmtop, PDAs, and other transportable computers containing sensitive information must not check these computers in airline luggage systems. To avoid damage and theft, these computers must remain in the possession of the traveler as hand luggage.

15. Appendix 7 – Backup and Disaster Recovery Approach

15.1 Introduction

The disaster recovery plan identifies the processes that are critical to the business along with the resources and data associated with these processes. The plan outlines the necessary recovery objectives for these processes and resources in the event of a natural or human caused disaster.

This document describes the Disaster Recovery Plan that the IT department will use in the event that a disaster affects the organization's operations and services. It includes a summary of the current services, identification of the services most critical to company operations, and how these services will be reconstituted following a disaster.

15.2 Scope of this Plan

This plan provides the IT department with the ability to address the following areas:

- It enables the department to restore TopSource's core information systems in the event of a disaster.
- It identifies areas of substantial risk and exposure to disaster, and helps to reduce these risks.

This plan is not intended to be a detailed, step by step series of instructions to follow. Rather, it is intended to be a roadmap to lead the recovery team with informed decision making to implement the restoration of services. Although it is targeted at the most likely types of disasters that could be encountered, it may be adapted as necessary for recovery from other situations.

15.3 Current Practices & Procedures

An understanding of the operational practices currently followed by the IT department is essential to recovering systems and applications. The key activities include:

- Data backup & restoration
- Identification of critical systems

Data Backup & Restoration

Full backups of all servers are performed on offsite server quarterly. The daily incremental backup is restored on an off-site backup server every day.

A restore drill procedure is followed once every 3 months with the backup from off-site server

brought into the offices to restore and test the backup.

For further information on Server backup & restore procedure please refer Backup & Disaster recovery Policy for Topsource.

16. Appendix 8 – Managing 3rd Party Contractors

16.1 Introduction

This policy is internal to TOPSOURCE and it defines the approach for managing 3rd party contractors / vendors.

16.2 Purpose

This policy specifies controls to reduce the information security risks associated with using 3rd party contractors. The policy applies to all departments in TopSource that may require the use of 3rd party contractors.

3rd Party contactors (also known as outsourcers)/ vendors will include:

- Hardware and software support and maintenance staff
- External consultants and contractors
- IT or business process outsourcing firms
- Temporary staff suppliers

The policy addresses the following controls

- Identification of risks related to external parties
- Addressing security when dealing with customers
- Addressing security in third party agreements

16.3 Managing 3rd Party Contactor Policy

The organization will use following procedure for choosing new vendors and providing access to office premises to existing 3rd party contractors/vendors.

16.3.1 Choosing a 3rd Party Contractor

Criteria for selecting a vendor/contractor should take into account the following:

- Vendor's reputation and history
- Quality of services provided to other customers
- Financial stability of the company and commercial record

- Quality assurance and security management standards currently followed by the vendor

16.3.2 Assessing risks

In relation to outsourcing to 3rd party contractors, the risk assessment shall take due account of the following:

- Nature of logical and physical access to information assets and facilities required by the outsourcer to fulfill the contract.
- Sensitivity, volume and value of any information assets involved
- Commercial risks such as the possibility of the outsourcer's business failing completely, or of them failing to meet agreed service levels or providing services and security

The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract.

16.3.3 Contracts and confidentiality agreements

A formal contract or Purchase Order/Quotation between TopSource and the 3rd party vendor shall exist to protect both parties. The contract shall clearly define the types of information exchanged and the purpose for so doing.
If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between TopSource and the vendor, whether as part of the outsource contract itself or a separate non-disclosure agreement.
Information shall be classified and controlled in according with TopSource data classification policy.

Any information received by TopSource from the vendor/3rd party contractor which is bound by the contract or confidentiality agreement shall be protected by appropriate classification and labeling.

Upon termination of the contract, the confidentiality arrangements shall be revisited to determine whether confidentiality has to be extended beyond the tenure of the contract.

The contract shall clearly define each party's responsibilities toward the other by defining the parties to the contract, effective date, functions or services being provided (e.g. defined service levels), liabilities, limitations on use of sub-contractors and other commercial/legal matters normal to any contract. Depending on the results of the risk assessment, various additional controls should be embedded or referenced within the contract.

Suitable information security awareness, training and education shall be provided to all employees and third parties working on the contract, clarifying their responsibilities relating to TopSource information security policies, standards, procedures and guidelines (e.g. privacy

policy, acceptable use policy, procedure for reporting information security incidents etc.) and all relevant obligations defined in the contract.

16.3.4 Access controls

In order to prevent unauthorized access to TopSource's information assets by the vendor or sub-contractors, suitable security controls are required as outlined in this section. The details depend on the nature of the information assets and the associated risks, implying the need to assess the risks and design suitable controls architecture.

Access controls shall include:

- User identification and authentication
- Authorization of access, generally through the assignment of users to defined user roles having appropriate logical access rights and controls
- Accounting/audit logging of access checks, plus alarms/alerts for attempted access violations where applicable
- Access logging though the use of access cards, visitor registers etc.

17. Appendix 9 - Social Networking media acceptable usage policy.

17.1 Introduction

Social media refers to the means of interactions among people in which they create, share, and exchange information and ideas in virtual communities and networks. Social media includes any Web site in which visitors are able to publish content to a larger group. Content shared may include (but is not limited to) personal information, opinions, research, commentary, video, pictures, or business information. Examples of such destinations include large branded entities such as Facebook, Twitter, YouTube, and LinkedIn. However, blogs, special interest forums, user communities are also considered social media.

17.2 Purpose

Social media offers important business advantages to companies and organizations, but also has well-known security risks. In order to mitigate these security risks and still enjoy the benefits of social media organizations must establish and enforce good social media usage policy.

17.3 Inappropriate Content Policy

While social media contains legitimate business and personal content, they also include content that is inappropriate for the workplace including nudity, violence, abused drugs, sex, and gambling. Therefore, the same inappropriate content policy that applies to the broader Web, also applies to content found within social media. Inappropriate content should not be accessed by employees while at work, or while using company resources. In addition to these guidelines, employees should use common sense and consideration for others in deciding which content is appropriate for the workplace.

17.4 Content Publishing and Confidentiality Policy

The following are policy guidelines regarding what you should and should not do when publishing content in social media. These guidelines apply to all social media communications whether personal or company-sponsored. Employees are responsible for content they publish in social media and can be held personally liable for content published. Employees also can be subject to disciplinary action by TopSource for publishing inappropriate or confidential content. These guidelines only cover a sample of all possible content publishing scenarios and are not a substitute for good judgment.

- DO know and follow all privacy and confidentiality guidelines in the Employee Handbook. All guidelines in the employee handbook, as well as laws such as copyright, fair use and financial disclosure laws apply to social media.
- DO NOT disclose or use TopSource confidential or proprietary information or that of any other person or company. For example, ask permission before posting someone's picture in a social network or publishing in a blog a conversation that was meant to be private.
- DO identify yourself. Some individuals work anonymously, using pseudonyms or false screen names. TopSource discourages that practice.
- If you have identified yourself as a TopSource employee within a social website, you are connected to your colleagues, managers and even TopSource customers. You should ensure that content associated with you is consistent with your work at TopSource
- When you do make a reference to a customer, partner or supplier, where possible link back to the source.
- If you identify yourself as a TopSource employee, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and customers.
- DO NOT use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the TopSource workplace. You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory.
- DO NOT conduct confidential business with a customer or partner business through your personal or other social media.
- DO NOT register accounts using the TopSource brand name or any other unregistered or registered trademarks.

17.5 Social networking sites for Topsource –

Below are links to our social media networking sites. Please do take some time out over the weekend to visit our social networking platforms for the TopSource and Portico brands and click your 'likes', start following and communicate the same to your friends and acquaintances. The links are provided below.

This is all part of the groundwork that we need to do to build a community around our service offering and products.

	TopSource Worldwide
Twitter	https://twitter.com/TopSourceWW
Linked In	https://www.linkedin.com/company/topsource-worldwide
	TopSource UK
Facebook	https://www.facebook.com/topsourceuk
Twitter	https://twitter.com/topsourceuk
Linked In	http://www.linkedin.com/company/topsource-global-solutions
Google Plus	https://plus.google.com/108836069765388888729
Vimeo	http://vimeo.com/groups/porticouk
YouTube	http://www.youtube.com/user/porticouk

	TopSource India
Facebook	https://www.facebook.com/topsource.in
Twitter	https://twitter.com/topsourcein
Linked In	http://www.linkedin.com/company/topsource-india
Google Plus	https://plus.google.com/105365556956434944938

	Portico UK
Facebook	https://www.facebook.com/porticoUK
Twitter	https://twitter.com/portico_uk
Linked In	http://www.linkedin.com/company/portico-uk
Google Plus	https://plus.google.com/114087495527265703399

Should you have any feedback, please feel free to share with us

18. Appendix 10 – Server Security Policy

18.1 Introduction

An organization's servers provide a wide variety of services to internal and external users, and many servers also store or process sensitive information for the organization. Some of the most common types of servers are Web, email, database, infrastructure management, and file servers.

This policy defines the general procedure followed in TopSource to address security issues of typical servers.

18.2 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by TopSource .Effective implementation of this policy will prevent unauthorized access to TopSource proprietary information and technology.

18.3 Scope

This policy applies to all authorized servers owned and configured within the TopSource offices and operated from hosted network.

18.4 Physical security

- All servers will be hosted within dedicated server rooms.
- All server rooms will have secure perimeters.
- All server rooms will have access restricted by Access Control system and additionally by lock keys. Access will be limited to members of IT Team and Business Unit Director (additional access is provided to Security team for emergency).
- All servers will be marked with an individual system tag and the server name.

18.5 Environment Security

- All servers will be protected from surges, spikes, sags or brownouts in the electricity supply by the use of Uninterruptible Power Supplies.
- All servers will be situated in racks, raising them above ground level and therefore reducing the liability of damage through flooding.
- Server room will have separate air conditioning equipment and will be fitted with dust filters

18.6 Logical Security

- Access to server operating systems shall only be granted to IT Team.
- Access to applications and storage spaces shall be tightly controlled by the use of Access Control Lists.
- Remote access to server operating systems shall only be granted by default to IT Team. Remote access may be granted to other authorized users on a case by case basis, where the request is made by the Project Manager and the request is approved by Business Unit Director.
- User access, where facilitated, will be provided on a basis of least privilege, tight Group Policy implementation, granular NTFS access controls and limited access to programs
- Use of utility programs is restricted to members of the IT Support Team.
- Server software and firmware will be patched in a timely manner. Non-critical and test systems will be patched first to test system and application operability.

18.7 Controls against Malicious Code

- Anti-virus software will be installed on every server and kept up-to-date.
- All servers will sit behind firewalls.
- User access to server desktop environments, where required for remote desktop purposes, will be tightly controlled by Group Policy in order to block access to system programs, tools, files and processes. User access will have no administrative rights, installation rights or elevated privileges.
- Internet Explorer will only run in Enhanced Security Configuration mode.

18.8 General Configuration Guidelines

- Operating System configuration should be in accordance with approved InfoSec guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use a privileged account for login to Linux operating system.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPsec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

19. Appendix 11 – Server and workstations Preventive maintenance

19.1 Introduction

This document is internal to TOPSOURCE and it defines the approach for carrying out Server and Workstation maintenance.

19.2 Purpose

This policy specifies checklist to follow while carrying out maintenance for Servers as well as workstations.

19.2.1 Preventive Maintenance Checklist for Servers

SERVER NAME:- **DATE:-**

No.	P. M.CHECKLIST	Done	REMARK
1	Physical cleaning of Server (Dust cleaning).		
2	Check that all the connections are secure e.g. power, network, etc.		
3	Check all the system logs (System, Applications, Security, Active Directory) for any warnings or errors and action accordingly.		
4	Remove all temp files and all temp internet files.		
5	Install Windows updates and patches. Restart server if needed.		
6	Check anti-virus logs and updates		
7	Check free disk space on all drives. (at least 15% disk space should be free on all drives)		
8	Check CPU and memory utilization. (CPU utilization should be below 50%)		
9	Check replication if server is domain controller.		
Report any suspicious activity / variation from default values to IT Manager			

ENGINEER NAME:-

REMARKS:- **ENGINEER SIGNATURE:-**

19.2.1 Preventive Maintenance Checklist for Workstations

COMPUTER NAME:-

No.	P. M.CHECKLIST	Done	Remark
1	Physical cleaning of PC (Dust cleaning).		
2	PC should be connected to UPS supply.		
3	Check if the Keyboard, Mouse and Monitor are in working condition.		
4	Remove all temp files and temp internet files.		
5	Set Virtual memory to 3000MB		
6	Windows firewall should be OFF.		
7	Check for proper working of VNC.		
10	Ensure that only required drives are mapped.		
11	Check last updated date & perform clean up through Quick Heal Antivirus		
12	Removal of unwanted Identities and its mail store after consulting the user and project manager.		
13	Ensure that there is a minimum of 1 GB free space on C: drive.		
14	Perform defragmentation of all drives.		
15	Create System Restore Point.		

ENGINEER NAME:-

REMARKS:- **ENGINEER SIGNATURE:-**

Appendix 20 – Removable Media Policy

20.1. Introduction

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

IT team will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting organization business.

20.2. Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by TopSource and to reduce the risk of acquiring malware infections on systems.

20.3. Removable Media Policy

Removable media devices include, but are not restricted to the following:

- CDs.
- DVDs.
- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- Backup Cassette

20.3.1 Restricted Access to Removable Media

It is TopSource's policy to prohibit the use of all removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

20.3. 2 Procurement of Removable Media

All removable media devices and any associated equipment and software must only be purchased and installed by IT Support team at TopSource. Other than organization owned removable media devices must not be used to store any information used to conduct official business, and must not be used with any TopSource owned or leased IT equipment.

20.3.3 Security of Data

In order to minimize physical risk, loss, theft or electrical corruption, all removable storage media must be stored in an appropriately secure and safe environment. Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way while in their care or under their control.

Appendix 21 – Remote work Policy

21.1 Introduction

This Remote work policy outlines the guidelines, rules, and procedures for employees who work remotely from a location other than offices. The remote work is a working style that allows professionals to work outside of a traditional office environment.

21.2. Purpose

This policy has been developed to protect sensitive or valuable data and maintain the overall security of data and equipment while employees are working remotely. It can act as a guide for both management and the employee.

21.3 Eligibility

TopSource provide equal opportunity to all its employees to be eligible for working remotely when unable to attend office and can execute the duties by remotely working. This also applies to certain pandemic conditions where in the office premises are not accessible.

21.4 Compliance with polices.

Our remote employees must follow all company policies like their office-based colleagues.

- Attendance
- Confidentiality
- Data protection
- Dress code when meeting in-person or by video call with colleagues & clients.

21.4 Remote work policy

- In case remote working is required, the practice manager would ensure that the team member working remotely will have the necessary connectivity and sufficient bandwidth to carry out the work remotely. The desktop/laptop that is used at workplace can be taken to remote location after getting the necessary permission and the clearance from the practice manager.
- The security personnel will check the approval before allowing movement of the desktop/laptop.
- The desktop/laptop will have the software to enable connection with the servers including VPN client, MS Teams, firewall, antivirus software. The IT team will ensure that desktop/laptop has the latest patches of the software.
- In case of hardware problems, the equipment needs to be brought back to the office for checking and then replacement.
- Inventory of machine in the office and outside office with remote connectivity is maintained by the IT team.